Remarks/Arguments

The Office Action dated November 12, 2004, the time to respond having been extended by separate petition to May 12, 2005, has been noted and its contents carefully studied. In light of the foregoing amendments and following comments, reconsideration of the Rejection under 35 U.S.C §103 is courteously requested.

To facilitate the Examiner's reconsideration, a brief discussion of the invention is presented herein. The claimed invention pertains to the specific field of user terminal digital storage and encryption to prevent further distribution of all recorded media through the user terminal to additional user terminals through distribution networks, such as the internet, LAN, WAN, etc. In one aspect as recited in independent claims 1 and 8, media content is received at the user terminal via any type of broadcast such as from a digital television broadcaster. A system and method encrypts the media at the user terminal, and <u>not</u> prior to transmission to the user terminal. Once encrypted, the content can only be played back or reviewed by the unique user terminal in which the media was originally received.

The process is implemented through a series of encryption steps before and within local storage, and reverses the encryption process, i.e., decryption, through the user terminal in which the media is stored after having been encrypted.

If during decryption, the claimed logic does not match the stored media content to the user terminal in which the media is stored, the logic within the user terminal will not play back or render the media content for display.

In operation as described and claimed, the user terminal initially receives and demodulates the broadcast media signal from the tuner and demodulator, creating a downloadable bit stream. From there, the user terminal places the downloaded bit stream into a wrapper, described as data that precedes the frames of the main data or program as seen in Figure 5. The created wrapper sets up the downloaded bit stream so that the next step in the encryption process can run successfully. The wrapped bit stream is sent to the input of a capture filter and it is in this filter where the eventual recording or storing of media content is arranged. Before leaving the capture filter for recording or storage, the capture filter randomly removes bits according to a certain encryption algorithm and each user terminal is assigned a unique identifier that dictates the unique encryption process. When the media content is encrypted prior to storage, the unique user terminal identifier is embedded and encrypted within the encryption process and stored within the stored or recorded media content.

The decryption process initiates when media is to be retrieved from the user terminal storage such as a hard drive, DVD or magnetic tape. The wrapper discussed previously is reversed and removed, creating an encrypted bit stream. The encrypted bit stream is identified for the point of origin and a check is made to ensure that encrypted bits contain the unique user terminal identification. If the process determines the retrieved content has a different point of origin other than the user terminal, the system determines what decision to make with the content, for example, the system may permanently delete the media content from the storage medium. Thus, the system and method prevents any distribution of recorded or stored media content beyond the user terminal which created the original stored media content.

It is respectfully urged that the invention as recited in the claims is not anticipated by or obvious under 35 U.S.C §102 and/or §103 from the cited references, as will become more readily apparent from the following detailed discussion of these references presented herein for the Examiner's kind consideration.

U.S. Patent No. 5,822,676 to Hayashi et al.

U.S. Patent No. 5,822,676 to Hayashi et al. (hereinafter "Hayashi") teaches a method and apparatus for including a serial number into a program, in which the encoder embeds the serial number into the program event so that it is imperceptible to the user when the program is rendered to the user. Hayashi uses a technique of embedding a unique serial number such that any storage medium storing the program can be traced back to the user. This encoding technique is especially useful in interactive systems where a server at the head end receives subscriber identification numbers along with subscriber requests for program events. The server can generate a serial number unique to the user for each requested program. A serial number can be generated through various means such as a time stamp, etc.

Hayashi fails to disclose or suggest the claimed invention. Hayashi in contrast to the invention teaches embedding the serial number at the head end server, and then broadcasts the program event within the cable plant. The inventors' claimed invention embeds a unique serial number at the user terminal, not at a head end server. The programs that the user terminal receives in accordance with the invention are not encrypted before consumption by the user terminal. In contrast, the programs received by Hayashi's terminals are already encrypted before consumption.

The claimed invention requires that a non-encrypted program be received and consequently uniquely encrypts the program at the user terminal prior to storage or recording.

U.S. Patent No. 5,995,625 to Sudia et al.

U.S. Patent No. 5,995,625 to Sudia et al. (hereinafter "Sudia") teaches a method of unwrapping wrapped digital data that is unusable while wrapped. The method includes obtaining an acceptance phrase from a user, deriving a cryptographic key from the acceptance phrase and unwrapping the package of digital data using the derived cryptographic key. In Sudia, like Hayashi, the end user obtains the digital data in wrapped form and the user must have the conditions and must enter the acceptance phrase in order to unwrap and then use the unwrapped data.

The claimed invention is completely opposite to that in that the program arrives totally unwrapped and unencrypted and is then later encrypted at the user terminal with the user encryption number embedded therein for later use by the user at the user terminal so that such programs cannot be distributed and used at other user terminals.

The remaining references have been reviewed and are not believed to be any more pertinent to the claimed invention than the aforementioned references. Thus, for sake of brevity they will not be discussed further herein.

For the foregoing reasons, it is respectfully urged that the all of the claims clearly define patentable subject matter under 35 U.S.C §102 and/or §103. Nonetheless, should the Examiner still have any comments, questions or suggestions of a nature necessary to expedite prosecution of the application, or to place the application in condition for allowance he is courteously requested to telephone the undersigned at the number listed below.

Dated: May 11, 2005

Respectfully submitted,

A. José Cortina, Reg. No. 29,733
Daniels Daniels & Verdonik, P.A.
P.O. Drawer 12218
Research Triangle Park, NC 27709
Voice 919.544.5444
Fax 919.544.5920
Email jcortina@d2vlaw.com

Enclosures

F:\CL\1213-003\Prosecution\Amendment.doc